WLR-2100/3100

Wireless Router N300

(802.11b/g/n)

User Manual

TABLE OF CONTENTS

1 KEY FEATURES 4
2 PACKAGE CONTENTS 5
3 CAUTIONS 6
4 PRODUCT LAYOUT 7
5 NETWORK + SYSTEM REQUIREMENTS 10
6 WLR-2100/3100 PLACEMENT 10
7 SETUP LAN, WAN 11
8 PC NETWORK ADAPTER SETUP 12
9 BRING UP THE WLR-2100/3100 16
10 INITIAL SETUP WLR-2100/3100 16
11 CONFIGURATION WIZARD 25
12 WIRELESS SETTINGS 27
13 FIREWALL SETTINGS 37
14 ADVANCED SETTINGS 43
15 TOOLBOX SETTINGS 50

Revision 1.0

© Sitecom Europe BV 2012

Note: All the information contained in this manual was correct at the time of publication.
However, as our engineers are always updating and improving the product, your device's software may have a slightly different appearance or modified functionality than presented in this manual.

Introduction

Congratulations on your purchase of the WLR-2100/3100 Wireless Network Broadband Router. The WLR-2100/3100 is compliant with 802.11n and up to 6 times faster than standard 802.11g based routers while still being compatible with 802.11g & 802.11b. The WLR-2100/3100 is not only a Wireless Access Point, but also doubles as a 4-port full-duplex Switch that connects your wired-Ethernet devices together.

At 300 Mbps wireless transmission rate, the Access Point built into the Router uses advanced MIMO (Multi-Input, Multi-Output) technology to transmit multiple steams of data in a single wireless channel, giving you seamless access to multimedia content. Robust RF signal travels farther, eliminates dead spots and extends network range. For data protection and privacy, the WLR-2100/3100 encodes all wireless transmissions with WEP, WPA, and WPA2 encryption.

With the inbuilt DHCP Server & powerful SPI firewall, the WLR-2100/3100 protects your computers against intruders and most known Internet attacks but provides safe VPN pass-through. With incredible speed and QoS function of 802.11n(draft2.0), the WLR-2100/3100 is ideal for media-centric applications like streaming video, gaming, and VoIP telephony to run multiple media-intense data streams through the network at the same time, with no degradation in performance.

The router includes Sitecom Cloud Security to protect your home network against cybercrime.

1 Key Features

Features	Advantages
Incredible Data Rate up to 300Mbps*	**Heavy data payloads such as MPEG video streaming**
IEEE 802.11n compliant and backwards compatible with 802.11b/g	**Fully Interoperable with IEEE 802.11b / IEEE802.11g compliant devices with legacy protection**
Four 10/100 Mbps Fast Switch Ports (Auto-Crossover)	**Scalability, extend your network.**
Firewall supports Virtual Server Mapping, DMZ, IP Filter, ICMP Blocking, SPI	**Avoids the attacks of Hackers or Viruses from Internet**
Support 802.1x authenticator, 802.11i (WPA/WPA2, AES), VPN pass-through	**Provide mutual authentication (Client and dynamic encryption keys to enhance security**
Sitecom Cloud Security	**Security integrated in the router protects all the devices in your network against cybercrime when surfing the Internet.**

** Theoretical wireless signal rate based on IEEE standard of 802.11a, b, g, n chipset used. Actual throughput may vary. Network conditions and environmental factors lower actual throughput rate. All specifications are subject to change without notice.*

2 Package Contents

Open the package carefully, and make sure that none of the items listed below are missing. Do not discard the packing materials, in case of return; the unit must be shipped back in its original package.

1. WLR-2100/3100 Router
2. 5V 1A Power Adapter
3. Quick Install Guide
4. CD (User's Manual)
5. Warranty card
6. UTP cable

3 Cautions

This router's design and manufacturer has your safety in mind. In order to safely and effectively use this router, please read the following before usage.

3.1 Usage Cautions

The user should not modify this router. The environmental temperature should be within +5 ~ +35 degrees Celsius.

3.2 Power

The router's power voltage is DC 5V 1A.
When using this router, please connect the supplied AC adapter or AC adapter cable to the router's power jack. When placing the adapter cable, make sure it can not get damaged or be subject to pressure. To reduce the risk of electric shock, unplug the adapter first before cleaning it. Never connect the adapter to the router in a humid or dusty area. Do not replace the adapter or cable's wire or connector.

3.3 Repair

If the router has a problem, you should take it to an appointed repair centre and let the specialists do the repair. Never repair the router yourself, you might damage the router or endanger yourself.

3.4 Disposing of the Router

When you dispose of the router, be sure to dispose it appropriately. Some countries may regulate disposal of an electrical device, please consult with your local authority.

3.5 Others

When using this router, please do not let it come into contact with water or other liquids. If water is accidentally spilled on the router, please use a dry cloth to absorb the spillage. Electronic products are vulnerable, when using please avoid shaking or hitting the router, and do not press the buttons too hard.

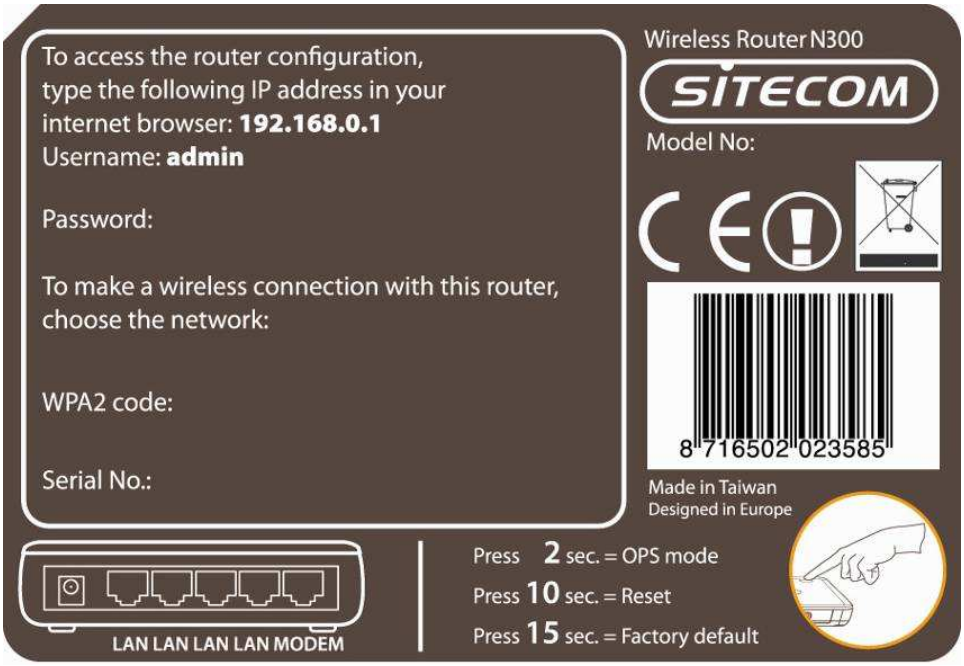
- Do not let the router come into contact with water or other liquid.
- Do not disassemble the router; repair the router or change the design of the router, any damage done will not be included in the repair policy.
- Avoid hitting the router with a hard object, avoid shaking the router and stay away from magnetic fields.
- If during electrostatic discharge or a strong electromagnetic field the product will malfunction, unplug the power cable. The product will return to normal performance the next time it is powered on.

4 Product Layout

Port	Description
Power connector	Connect the 5V DC adapter to this port
LAN (Yellow)	Connect your PC's or network devices to this port
WAN (Blue)	Connect your ADSL/Cable modem to this port

Backlabel

The backlabel describes the IP address, login details, SSID, security code and WPS button functionality.



Button	Description
WPS BUTTON	Press 2 seconds for WPS mode Press 10 seconds to reset the router Press 15 Seconds to reset the router to factory defaults.

LED Definition

From left to right.

Port	Description
LAN (Blue)	Shows the cable is connected.
LAN (Blue)	Shows the cable is connected.
LAN (Blue)	Shows the cable is connected.
LAN (Blue)	Shows the cable is connected.
WAN (Blue)	Shows the cable is connected.
WiFi (Blue)	Shows WiFi activity and WPS.
Power (Red)	Shows the device is turned on.

5 Network + System Requirements

To begin using the WLR-2100/3100, make sure you meet the following as minimum requirements:

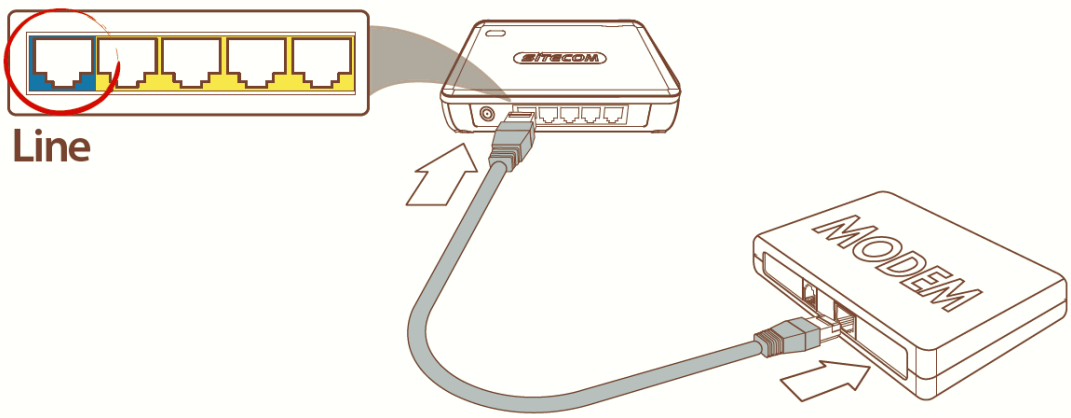
- PC/Notebook.
- Operating System – Microsoft Windows XP/VISTA/7
- 1 Free Ethernet port.
- WiFi card/USB dongle (802.11 b/g/n) – optional.
- External xDSL (ADSL) or Cable modem with an Ethernet port (RJ-45).
- PC with a Web-Browser (Internet Explorer, Safari, Firefox, Opera)
- Ethernet compatible CAT5 cables.

6 WLR-2100/3100 Placement

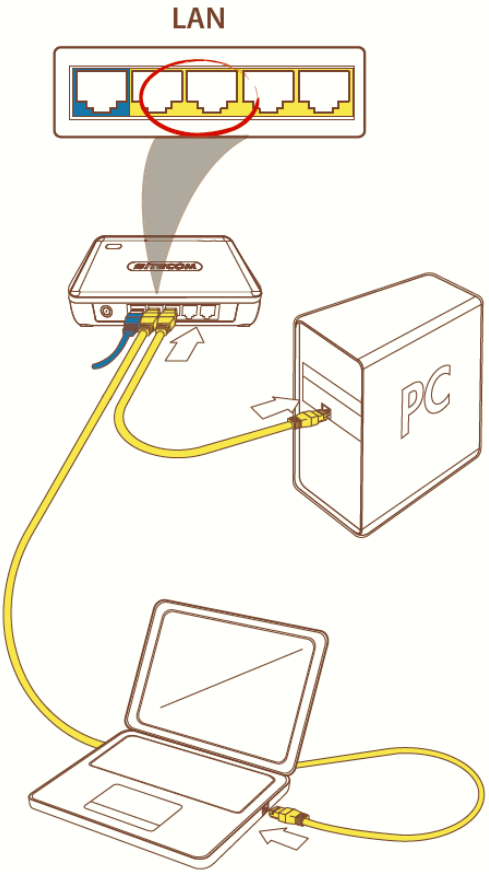
You can place the WLR-2100/3100 on a desk or other flat surface, or you can mount it on a wall. For optimal performance, place your Wireless Broadband Router in the center of your office (or your home) in a location that is away from any potential source of interference, such as a metal wall or microwave oven. This location must be close to a power connection and your ADSL/Cable modem.

7 Setup LAN, WAN

WAN connection:



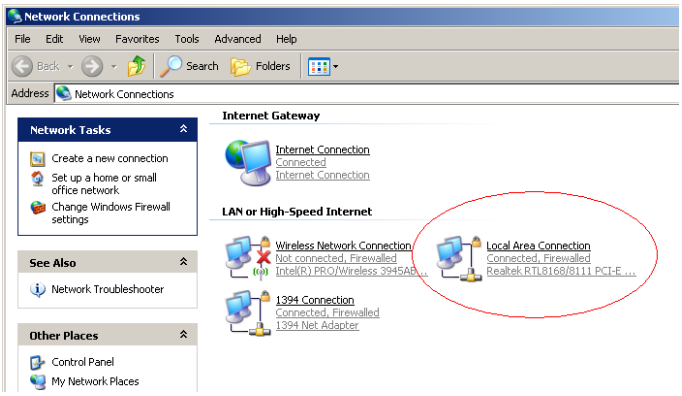
LAN connection:



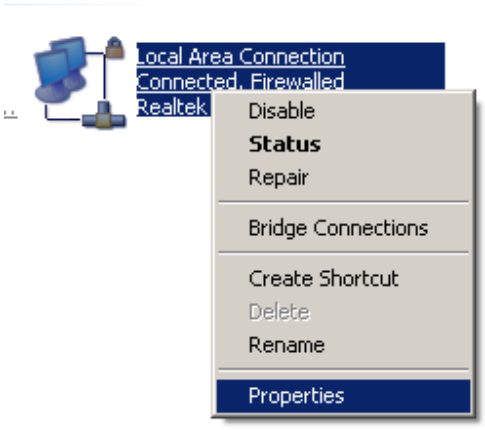
8 PC Network Adapter setup

Windows XP

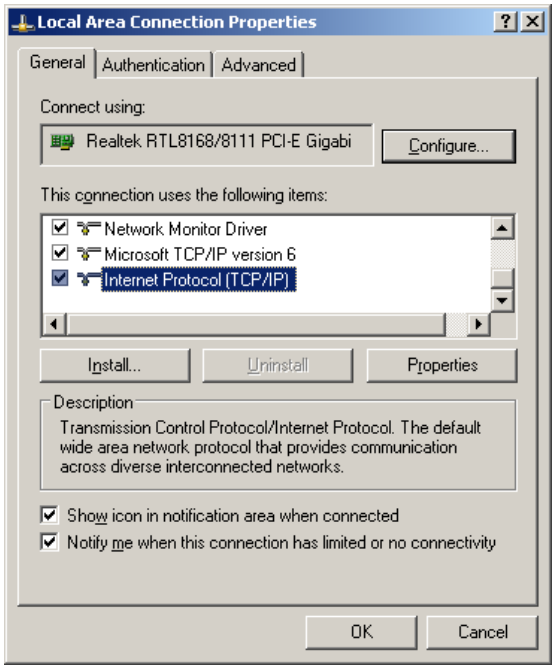
- Enter [Start Menu] → select [Control panel] → select [Network].

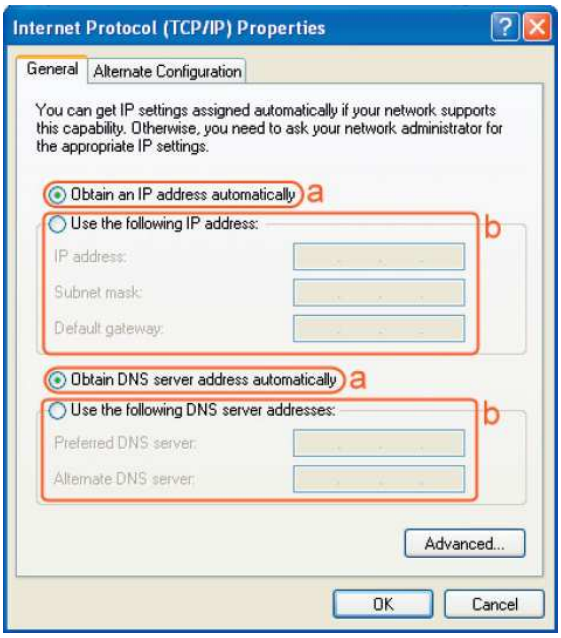


- Select [Local Area Connection]) icon=>select [properties]



- Select [Internet Protocol (TCP/IP)] =>Click [Properties].



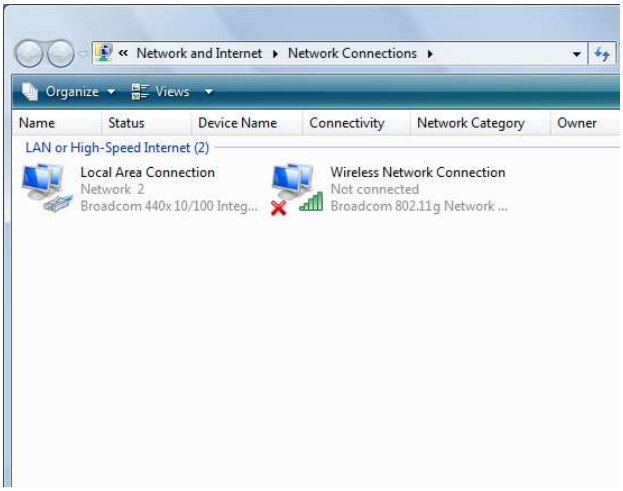


- Select the [General] tab.

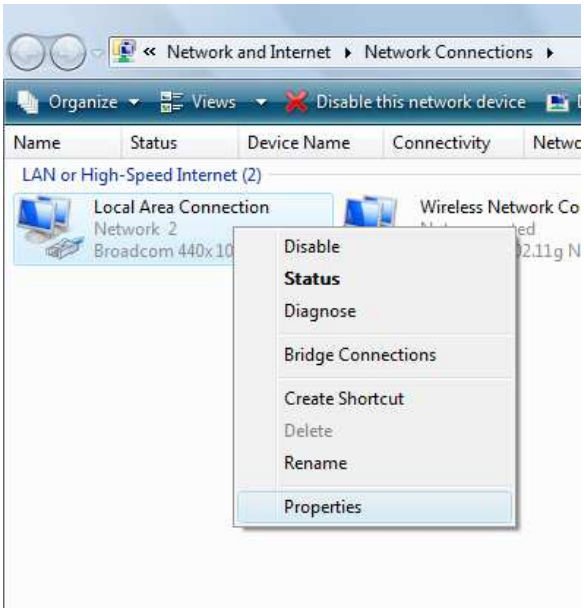
  The router supports [DHCP] function, please select both [Obtain an IP address automatically] and [Obtain DNS server address automatically].

Windows Vista/Seven

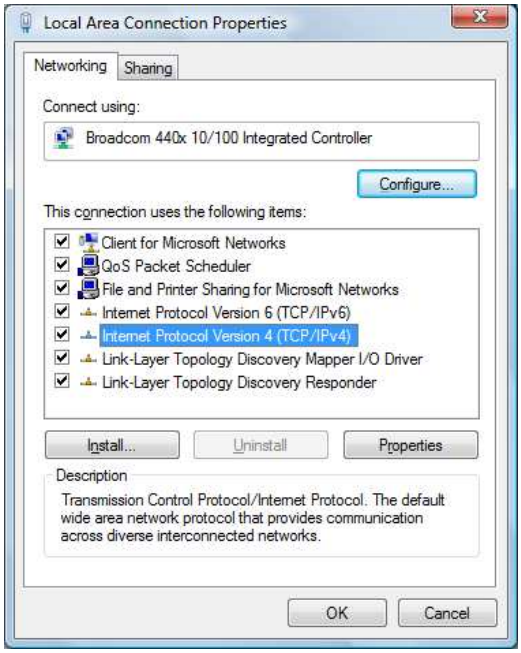
- Enter [Start Menu] → select [Control panel] → select [View network status and tasks] -> select [Manage network connections].

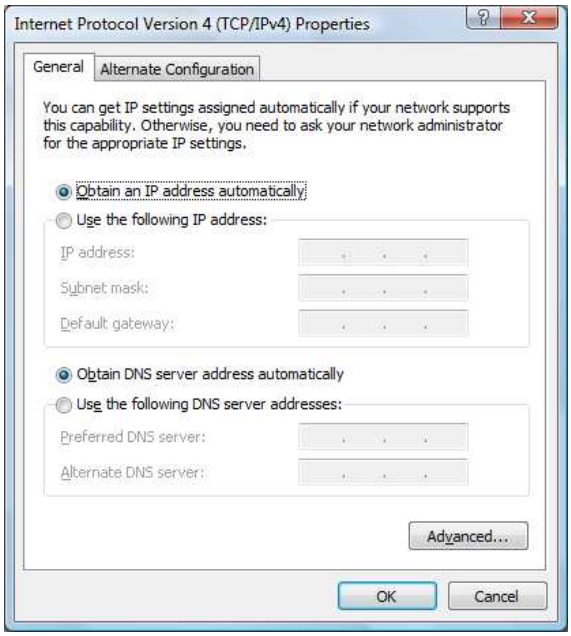


- Select [Local Area Connection]) icon=>select [properties]



- Select [Internet Protocol Version 4 (TCP/IPv4)] =>Click [Properties].




Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

- Select the [General] tab.

The router supports [DHCP] function, please select both [Obtain an IP address automatically] and [Obtain DNS server address automatically].

9 Bring up the WLR-2100/3100

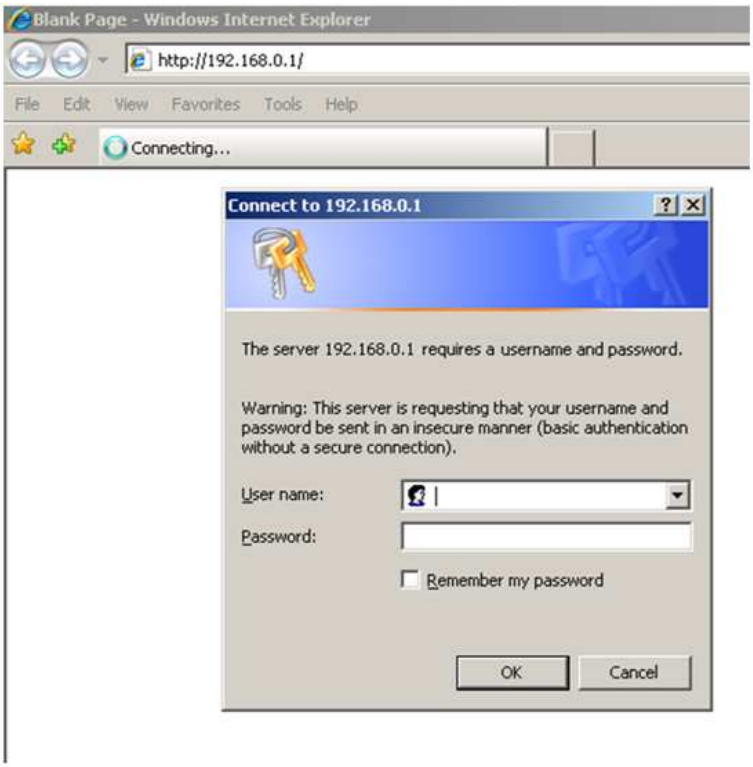
Connect the supplied power-adapter to the power inlet port and connect it to a wall outlet. The WLR-2100/3100 automatically enters the self-test phase. During self-test phase, the Power LED will be lit continuously to indicate that this product is in normal operation.

10 Initial Setup WLR-2100/3100

LOGIN procedure

1. OPEN your browser (e.g. Internet Explorer).

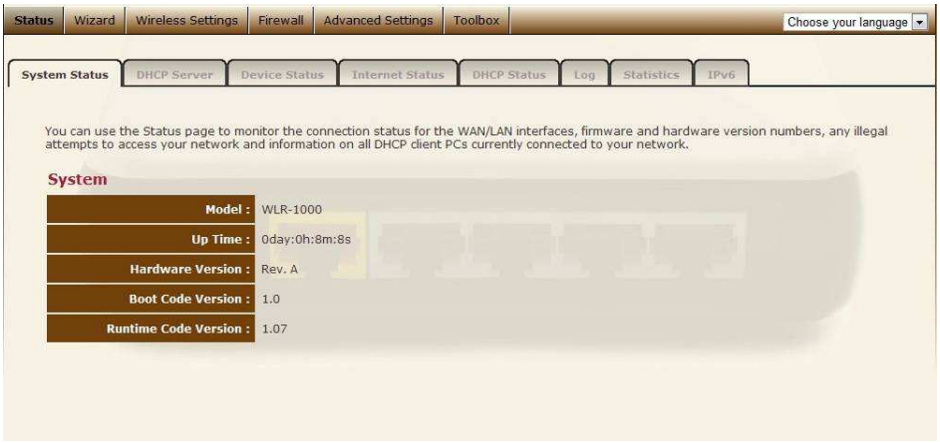
2. Type **http://192.168.0.1** in the address bar and press [Enter]


Blank Page - Windows Internet Explorer
http://192.168.0.1/
File Edit View Favorites Tools Help
Connecting...
Connect to 192.168.0.1
The server 192.168.0.1 requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
Password:
Remember my password
OK
Cancel

3. Type user name and password (default username is admin. The password can be found on the backlabel on the bottom of your router).

Connect to 192.168.0.1
The server 192.168.0.1 requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
admin
Password:
Remember my password
OK
Cancel

4. Click **OK**.
5. You will see the home page of the WLR-2100/3100.

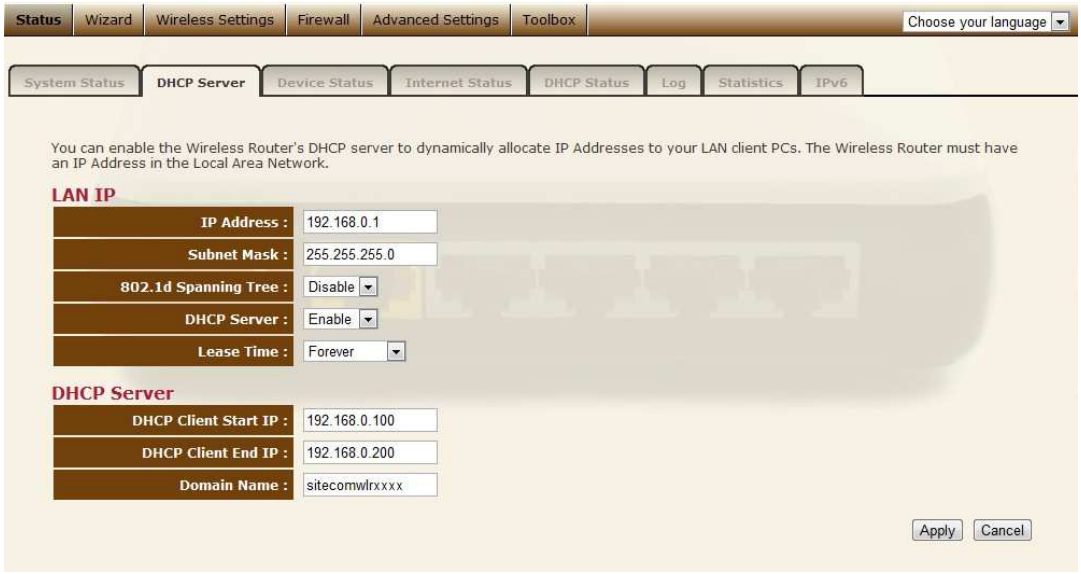


The System status section allows you to monitor the current status of your router.

The UP time, hardware information, serial number as well as firmware version information is displayed here.

DHCP Server

The LAN tab gives you the opportunity to change the IP settings of the WLR-2100/3100.



Click **<Apply>** at the bottom of this screen to save any changes.

IP address 192.168.0.1. It is the router's LAN IP address (Your LAN clients default gateway IP address).

IP Subnet Mask 255.255.255.0 Specify a Subnet Mask for your LAN segment.

802.1d Spanning Tree is Disabled by default. If the 802.1d Spanning Tree function is enabled, this router will use the spanning tree protocol to prevent network loops.

DHCP Server Enabled by default. You can enable or disable the DHCP server. When DHCP is disabled no ip-addresses are assigned to clients and you have to use static ip-addresses. When DHCP server is enabled your computers will be assigned an ip-address automatically until the lease time expires.

Lease Time Forever. In the Lease Time setting you can specify the time period that the DHCP lends an IP address to your LAN clients. The DHCP will change your LAN client's IP address when this time threshold period is reached.

DHCP START client IP/DHCP Client end IP You can select a particular IP address range for your DHCP server to issue IP addresses to your LAN Clients.
Note: default IP range 192.168.0.100 ←→ 192.168.0.200. If you want your PC(s) to have a static/fixed IP address, then you'll have to choose an IP address outside this IP address Pool

Domain Name You can specify a Domain Name for your LAN. Or just keep the default (sitecomwlrxxxx).

Device Status

View the Broadband router's current configuration settings. Device Status displays the configuration settings you've configured in the Wizard / Basic Settings / Wireless Settings section.

Internet Status

This page displays whether the WAN port is connected to a Cable/DSL connection. It also displays the router's WAN IP address, Subnet Mask, and ISP Gateway as well as MAC address, the Primary DNS. Press **Renew** button to renew your WAN IP address.

DHCP Client Status

DHCP This page shows all DHCP clients (LAN PCs) currently connected to your network. The table shows the assigned IP address, MAC address and expiration time for each DHCP leased client. Use the Refresh button to update the available information.

You can check **Enable Static DHCP IP**. It is possible to add more static DHCP IPs.
They are listed in the table S**tatic DHCP Lease Table**. IP can be deleted at will from the table.

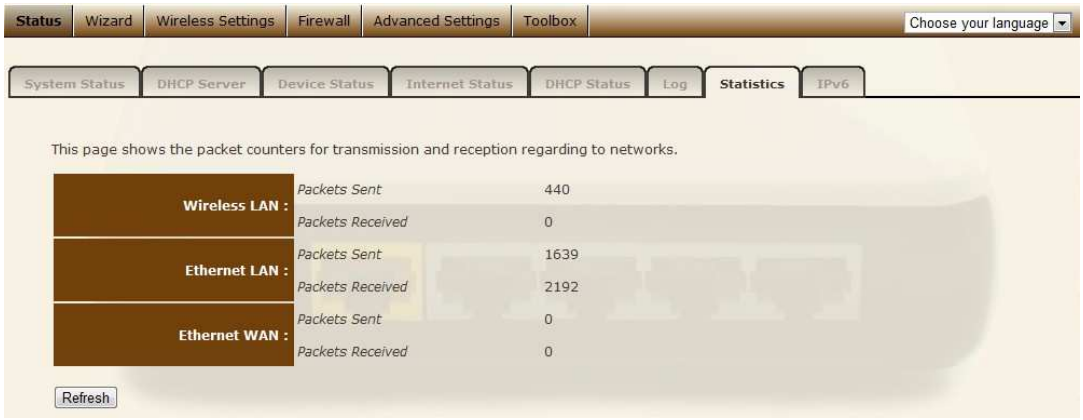
Click the '**apply'** button to save the changed configuration.

WLR-2100/3100 Log

View the operation **log of the WLR-2100/3100**. This page shows the current system log of the Broadband router. It displays any event occurred after system start up. At the bottom of the page, the system log can be saved **<Save>** to a local file for further processing or the system log can be cleared **<Clear>** or it can be refreshed **<Refresh>** to get the most updated information. When the system is powered down, the system log will disappear if not saved to a local file.

WLR-2100/3100 Statistics

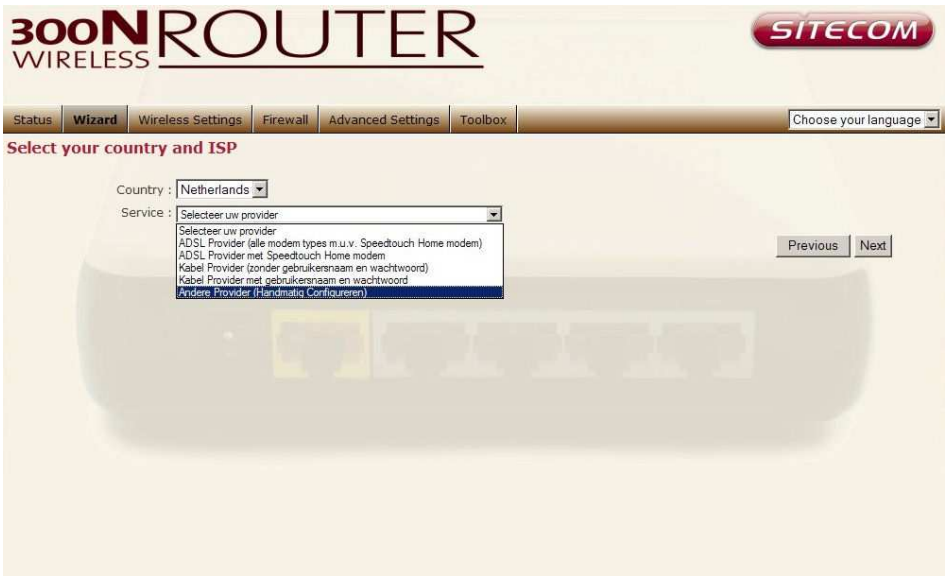
Shows the counters of packets sent and received on WAN, LAN & WLAN.



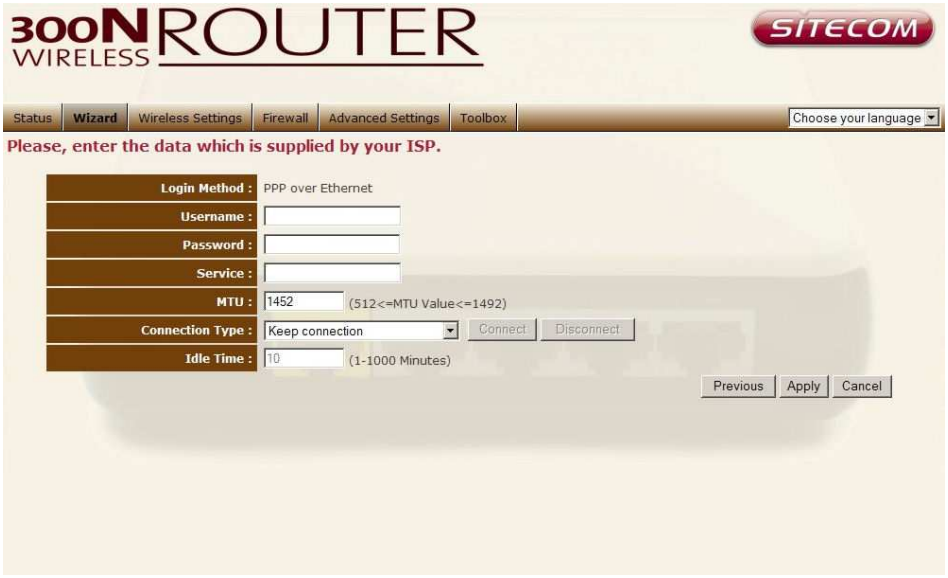
11 Configuration Wizard

Click **Wizard** to configure the router. The Setup wizard will now be displayed; check that the modem is connected and click **Next.**

Select your country from the Country list. Select your internet provider. Click **Next.**



Depending on the chosen provider, you may need to enter your user name and password, MAC address or hostname in the following window. After you have entered the correct information, click **Next**.



Click **APPLY** to complete the configuration.

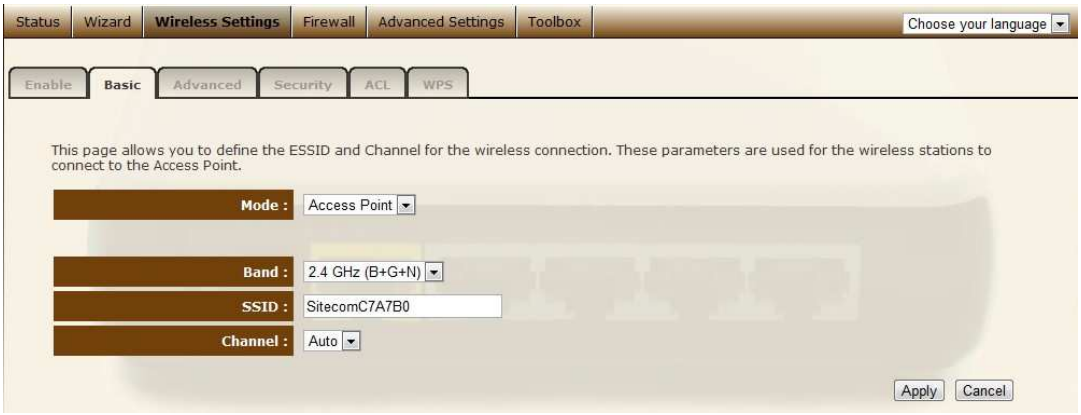
12 Wireless Settings

You can set parameters that are used for the wireless stations to connect to this router. The parameters include Mode, ESSID, Channel Number and Associated Client.

Wireless Function

Enable or Disable Wireless function here. Click **Apply** and wait for module to be ready and loaded.

Basic Settings



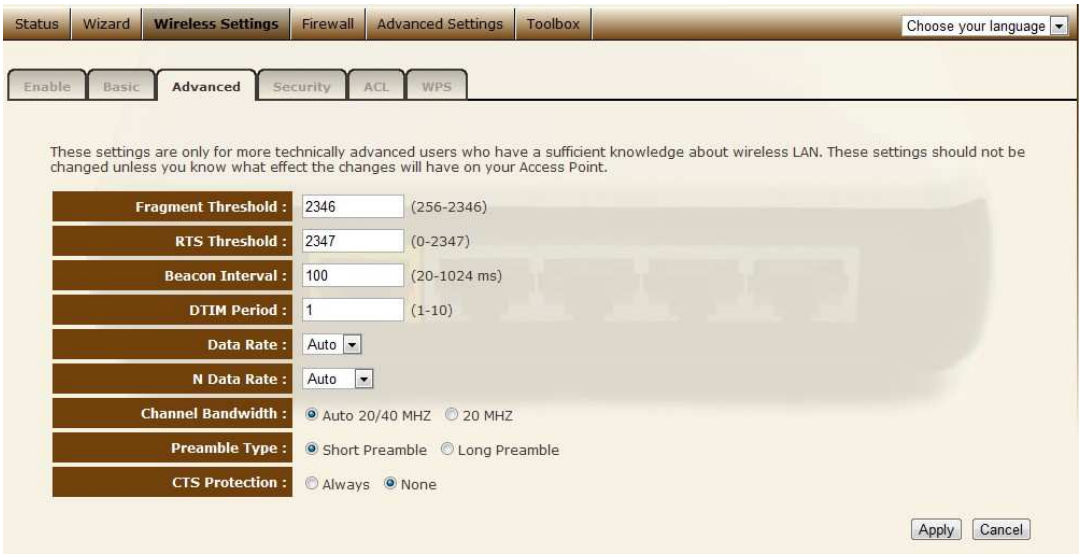
Band Allows you to set the AP fixed at 802.11b or 802.11g mode. You can also select B+G mode to allow 80211b and 802.11g clients at the same time.

SSID This is the name of the wireless signal which is broadcasted. All the devices in the same wireless LAN should have the same SSID.

Channel The channel used by the wireless LAN. All devices in the same wireless LAN should use the same channel.

Advanced

This tab allows you to set the advanced wireless options. The options included are, Fragment Threshold, RTS Threshold, Beacon Interval, and Preamble Type. You should not change these parameters unless you know what effect the changes will have on the router.


Status
Wizard
Wireless Settings
Firewall
Advanced Settings
Toolbox
Choose your language
Enable
Basic
Advanced
Security
ACL
WPS
These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.
Fragment Threshold : 2346 (256-2346)
RTS Threshold : 2347 (0-2347)
Beacon Interval : 100 (20-1024 ms)
DTIM Period : 1 (1-10)
Data Rate : Auto
N Data Rate : Auto
Channel Bandwidth : Auto 20/40 MHZ 20 MHZ
Preamble Type : Short Preamble Long Preamble
CTS Protection : Always None
Apply
Cancel

Fragment Threshold "Fragment Threshold" specifies the maximum size of a packet during the fragmentation of data to be transmitted. If you set this value too low, it will result in bad performance.

RTS Threshold When the packet size is smaller then the RTS threshold, the wireless router will not use the RTS/CTS mechanism to send this packet.

Beacon Interval is the interval of time that this wireless router broadcasts a beacon. A Beacon is used to synchronize the wireless network.

Data Rate The "Data Rate" is the rate that this access point uses to transmit data packets. The access point will use the highest possible selected transmission rate to transmit the data packets.

N Data Rate The "Data Rate" is the rate that this access point uses to transmit data packets for N compliant wireless nodes. Highest to lowest data rate can be fixed.

Channel Bandwidth is the range of frequencies that will be used.

Preamble Type The "Long Preamble" can provide better wireless LAN compatibility while the "Short Preamble" can provide better wireless LAN performance.

CTS Protection: It is recommended to enable the protection mechanism. This mechanism can decrease the rate of data collision between 802.11b and 802.11g wireless stations. When the protection mode is enabled, the throughput of the AP will be a little lower due to a lot of frame-network that is transmitted.

Security

This Access Point provides complete wireless LAN security functions, included are WEP, IEEE 802.11x, IEEE 802.11x with WEP, WPA with pre-shared key and WPA with RADIUS. With these security functions, you can prevent your wireless LAN from illegal access. Please make sure your wireless stations use the same security function, and are setup with the same security key.

Disable

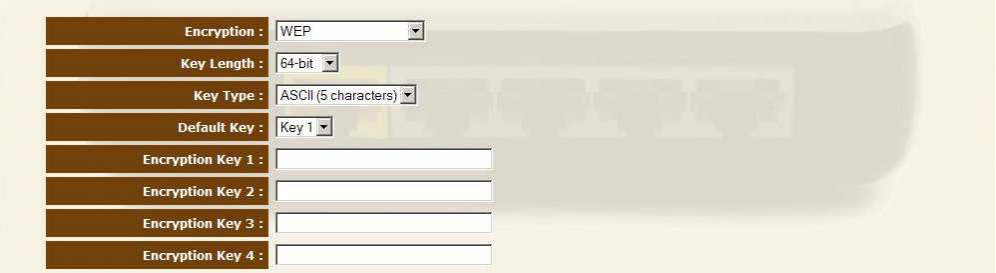
When you choose to disable encryption, it is very insecure to operate the WLR-2100/3100.

WPA Radius

IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates users by IEEE 802.1x, but it does not encrypt the data during communication

WEP

When you select 64-bit or 128-bit WEP key, you have to enter WEP keys to encrypt data. You can generate the key by yourself and enter it. You can enter four WEP keys and select one of them as a default key. Then the router can receive any packets encrypted by one of the four keys.



Key Length You can select the WEP key length for encryption, 64-bit or 128-bit. The larger the key will be the higher level of security is used, but the throughput will be lower.

Key Format You may select ASCII Characters (alphanumeric format) or Hexadecimal Digits (in the "A-F", "a-f" and "0-9" range) to be the WEP Key.

Key1 - Key4 The WEP keys are used to encrypt data transmitted in the wireless network. Use the following rules to setup a WEP key on the device. 64-bit WEP: input 10-digits Hex values (in the "A-F", "a-f" and "0-9" range) or 5-digit ASCII character as the encryption keys. 128-bit WEP: input 26-digit Hex values (in the "A-F", "a-f" and "0-9" range) or 13-digit ASCII characters as the encryption keys.

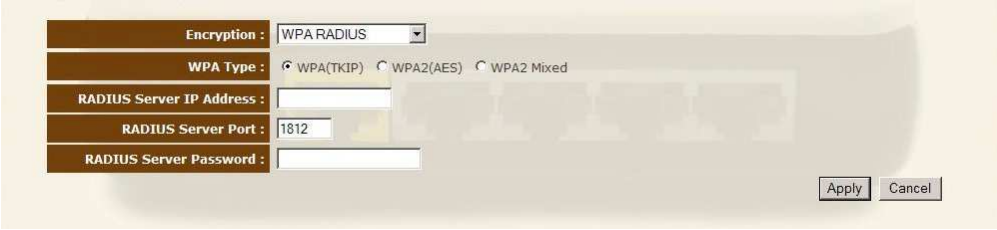
Click <Apply> at the bottom of the screen to save the above configurations. You can now configure other sections by choosing Continue, or choose Apply to apply the settings and reboot the device.

WPA Pre-shared Key

Wi-Fi Protected Access (WPA) is an advanced security standard. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently. So the encryption key is not easy to be cracked by hackers. This is the best security available.

WPA-Radius

Wi-Fi Protected Access (**WPA**) is an advanced security standard. You can use an external RADIUS server to authenticate wireless stations and provide the session key to encrypt data during communication. It uses **TKIP** or CCMP (**AES**) to change the encryption key frequently. Press **Apply** button when you are done.



ACL

This wireless router supports MAC Address Control, which prevents unauthorized clients from accessing your wireless network.

Enable wireless access control Enables the wireless access control function

Adding an address into the list Enter the "MAC Address" and "Comment" of the wireless station to be added and then click "Add". The wireless station will now be added into the "Current Access Control List" below. If you are having any difficulties filling in the fields, just click "Clear" and both "MAC Address" and "Comment" fields will be cleared.

Remove an address from the list If you want to remove a MAC address from the "Current Access Control List ", select the MAC address that you want to remove in the list and then click "Delete Selected". If you want to remove all the MAC addresses from the list, just click the "Delete All" button. Click "Reset" will clear your current selections.

Click <Apply> at the bottom of the screen to save the above configurations. You can now configure other sections by choosing Continue, or choose Apply to apply the settings and reboot the device.

WPS

Wi-Fi Protected Setup (WPS) is the simplest way to establish a connection between the wireless clients and the wireless router. You don't have to select the encryption mode and fill in a long encryption passphrase every time when you try to setup a wireless connection. You only need to press a button on both wireless client and wireless router, and WPS will do the rest for you.

The wireless router supports two types of WPS: WPS via Push Button and WPS via PIN code. If you want to use the Push Button, you have to push a specific button on the wireless client or in the utility of the wireless client to start the WPS mode, and switch the wireless router to WPS mode. You can simply push the WPS button of the wireless router, or click the 'Start to Process' button in the web configuration interface. If you want to use the PIN code, you have to know the PIN code of the wireless client and switch it to WPS mode, then fill-in the PIN code of the wireless client through the web configuration interface of the wireless router.

WPS Check the box to enable WPS function and uncheck it to disable the WPS function.

WPS Current Status If the wireless security (encryption) function of this wireless router is properly set, you'll see a 'Configured' message here. Otherwise, you'll see 'UnConfigured'.

Self Pin Code This is the WPS PIN code of the wireless router. You may need this information when connecting to other WPS-enabled wireless devices.

SSID This is the network broadcast name (SSID) of the router.

Authentication Mode It shows the active authentication mode for the wireless connection.

Passphrase Key It shows the passphrase key that is randomly generated by the wireless router during the WPS process. You may need this information when using a device which doesn't support WPS.

WPS via Push Button Press the button to start the WPS process. The router will wait for the WPS request from the wireless devices within 2 minutes.

WPS via PIN You can fill-in the PIN code of the wireless device and press the button to start the WPS process. The router will wait for the WPS request from the wireless device within 2 minutes.

13 Firewall Settings

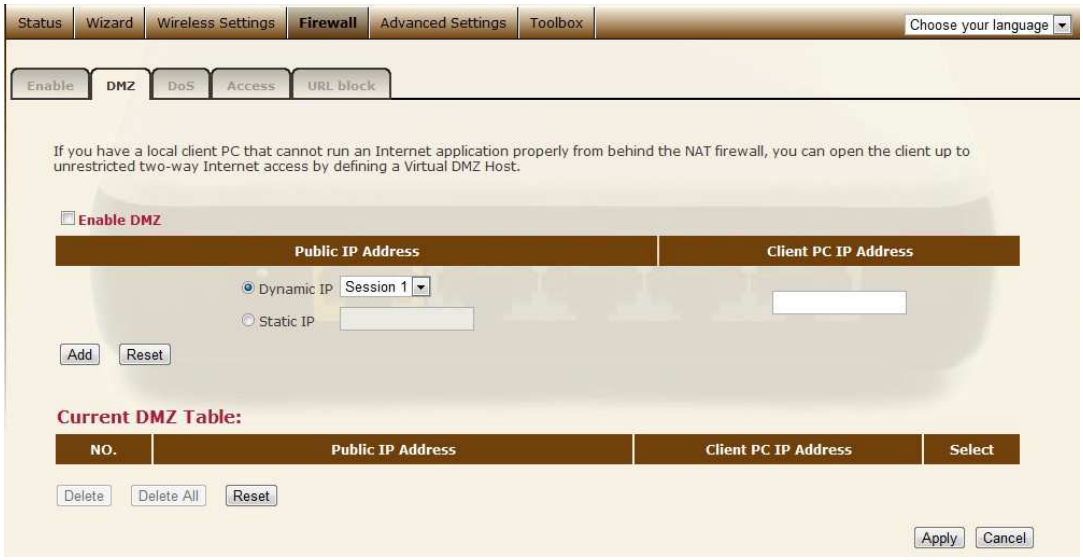
The Broadband router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attacks, and defending against a wide array of common Internet attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a Demilitarized Zone (DMZ).

Note: To enable the Firewall settings select Enable and click Apply

Status
Wizard
Wireless Settings
Firewall
Advanced Settings
Toolbox
Choose your language
Enable
DMZ
DoS
Access
URL block
The Wireless Router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attack, and defending against a wide array of common attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a Demilitarized Zone (DMZ).
Firewall Module:
Enable
Disable
Apply

DMZ

If you have a client PC that cannot run an Internet application (e.g. Games) properly from behind the NAT firewall, then you can open up the firewall restrictions to unrestricted two-way Internet access by defining a DMZ Host. The DMZ function allows you to re-direct all packets going to your WAN port IP address to a particular IP address in your LAN. The difference between the virtual server and the DMZ function is that the virtual server re-directs a particular service/Internet application (e.g. FTP, websites) to a particular LAN client/server, whereas DMZ re-directs all packets (regardless of services) going to your WAN IP address to a particular LAN client/server.



Enable DMZ Enable/disable DMZ

Public IP Address The IP address of the WAN port or any other Public IP addresses given to you by your ISP

Client PC IP Address Fill-in the IP address of a particular host in your LAN that will receive all the packets originally going to the WAN port/Public IP address above.

Click **<Apply>** at the bottom of the screen to save the above configurations.

Denial of Service (DoS)

The Broadband router's firewall can block common hacker attacks, including Denial of Service, Ping of Death, Port Scan and Sync Flood. If Internet attacks occur the router can log the events.

Ping of Death Protections from Ping of Death attack

Discard Ping From WAN The router's WAN port will not respond to any Ping requests

Port Scan Protects the router from Port Scans.

Sync Flood Protects the router from Sync Flood attack.

Access

You can restrict users from accessing certain Internet applications/services (e.g. Internet websites, email, FTP etc.), Access Control allows users to define the traffic type permitted in your LAN. You can control which PC client can have access to these services.

Deny If you select "Deny" then all clients will be allowed to access Internet accept for the clients in the list below.

Allow If you select "Allow" then all clients will be denied to access Internet accept for the PCs in the list below.

Filter client PCs by IP Fill in "IP Filtering Table" to filter PC clients by IP.

Add PC You can click Add PC to add an access control rule for users by IP addresses.

Remove PC If you want to remove some PCs from the "IP Filtering Table", select the PC you want to remove in the table and then click "Delete Selected". If you want to remove all PCs from the table, just click the "Delete All" button.

Filter client PC by MAC Check “Enable MAC Filtering” to enable MAC Filtering.

Add PC Fill in “Client PC MAC Address” and “Comment” of the PC that is allowed to access the Internet, and then click “Add”. If you find any typo before adding it and want to retype again, just click "Reset" and the fields will be cleared.

Remove PC If you want to remove some PC from the "MAC Filtering Table", select the PC you want to remove in the table and then click "Delete Selected". If you want to remove all PCs from the table, just click the "Delete All" button. If you want to clear the selection and re-select again, just click “Reset”.

Click <**Apply**> at the bottom of the screen to save the above configuration.

URL block

You can block access to some Web sites from particular PCs by entering a full URL address or just keywords of the Web site.

Enable URL Blocking Enable/disable URL Blocking

Add URL Keyword Fill in "URL/Keyword" and then click "Add". You can enter the full URL address or the keyword of the web site you want to block.

Remove URL Keyword If you want to remove some URL keywords from the "Current URL Blocking Table", select the URL keyword you want to remove in the table and then click "Delete Selected". If you want remove all URL keywords from the table, just click "Delete All" button. If you want to clear the selection and re-select again, just click "Reset".

Click <**Apply**> at the bottom of the screen to save the above configurations

14 Advanced Settings

Network Address Translation (NAT) allows multiple users at your local site to access the Internet through a single Public IP Address or multiple Public IP Addresses. NAT provides Firewall protection from hacker attacks and has the flexibility to allow you to map Private IP Addresses to Public IP Addresses for key services such as Websites and FTP. Select Disable to disable the NAT function.

Port Forwarding

Port Forwarding allows you to re-direct a particular range of service port numbers (from the Internet/WAN Port) to a particular LAN IP address. It helps you to host servers behind the router NAT firewall.

Enable Port Forwarding Enable Port Forwarding

Local IP This is the **local** IP of the server behind the NAT firewall.

Type This is the protocol type to be forwarded. You can choose to forward "TCP" or "UDP" packets only, or select "both" to forward both "TCP" and "UDP" packets.

Port Range The range of ports to be forward to the private IP.

Comment description of this setting.

Add Port Forwarding Fill in the "Private IP", "Type", "Port Range" and "Comment" of the setting to be added and then click "Add". Then this Port Forwarding setting will be added into the "Current Port Forwarding Table" below.

Remove Port Forwarding If you want to remove a Port Forwarding setting from the "Current Port Forwarding Table", select the Port Forwarding setting that you want to remove in the table and then click "Delete Selected". If you want to remove all Port Forwarding settings from the table, just click "Delete All" button. Click "Reset" will clear your current selections.

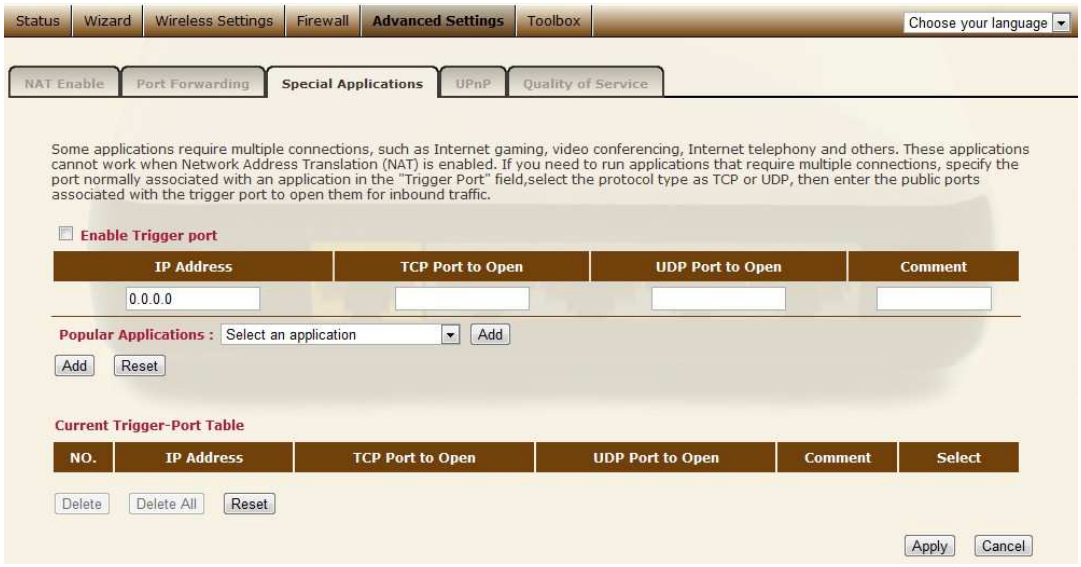
Special Applications

Some applications require multiple connections, such as Internet games, video Conferencing, Internet telephony and others. In this section you can configure the router to support multiple connections for these types of applications.

Enable Trigger Port Enable the Special Application function.

TCP Port to open This is the range of TCP port numbers for this particular application.

UDP Port to Open This is the range of UDP port numbers for this particular application.



Comment The description of this setting.

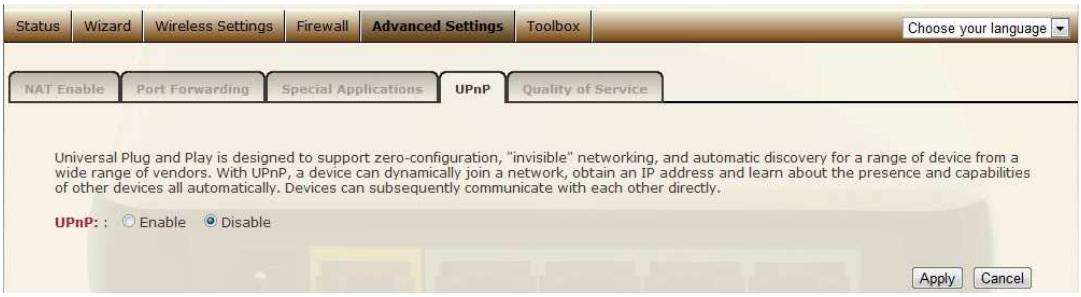
Popular applications This section lists the more popular applications that require multiple connections. Select an application from the Popular Applications selection. Once you have selected an application, select a location (1-10) in the Copy to selection box and then click the Copy to button. This will automatically list the Public Ports required for this popular application in the location (1-10) you specified.

Add Special Application Fill in the "Trigger Port", "Trigger Type", "Public Port", "Public Type", "Public Port" and "Comment" of the setting to be added and then click "Add". The Special Application setting will be added into the "Current Trigger-Port Table" below. If you happen to make a mistake, just click "Clear" and the fields will be cleared.

Delete If you want to remove Special Application settings from the "Current Trigger-Port Table", select the Special Application settings you want to remove in the table and then click "Delete Selected". If you want remove all Special Application settings from the table, just click the "Delete All" button. Click "Reset" will clear your current selections.

UPnP

With UPnP, all PCs in you Intranet will discover this router automatically, so you don't have to configure your PC and it can easily access the Internet through this router.


Status
Wizard
Wireless Settings
Firewall
Advanced Settings
Toolbox
Choose your language
NAT Enable
Port Forwarding
Special Applications
UPnP
Quality of Service
Universal Plug and Play is designed to support zero-configuration, "invisible" networking, and automatic discovery for a range of device from a wide range of vendors. With UPnP, a device can dynamically join a network, obtain an IP address and learn about the presence and capabilities of other devices all automatically. Devices can subsequently communicate with each other directly.
UPnP: : Enable Disable
Apply
Cancel

UPnP Feature You can enable or Disable the UPnP feature here. After you enable the UPnP feature, all client systems that support UPnP, like Windows XP, can discover this router automatically and access the Internet through this router without having to configure anything. The NAT Traversal function provided by UPnP can let applications that support UPnP connect to the internet without having to configure the virtual server sections.

QoS

QoS can let you classify Internet application traffic by source/destination IP address and port number. You can assign priority for each type of application and reserve bandwidth for it. The packets of applications with higher priority will always go first. Lower priority applications will get bandwidth after higher priority applications get enough bandwidth. This can let you have a better experience in using critical real time services like Internet phone, video conference …etc. All the applications not specified by you are classified as rule name "Others". The rule with a smaller priority number has a higher priority; the rule with a larger priority number has a lower priority. You can adjust the priority of the rules by moving them up or down.

Enable/Disable QoS You can check "Enable QoS" to enable QoS functionality for the WAN port.

Add a QoS rule into the table Click "Add" then enter a form of the QoS rule. Click "Apply" after filling out the form the rule will be added into the table.

Remove QoS rules from the table If you want to remove QoS rules from the table, select the QoS rules you want to remove in the table and then click "Delete Selected". If you want remove all QoS rules from the table, just click the "Delete All" button. Clicking "Reset" will clear your current selections.

Edit a QoS rule Select the rule you want to edit and click "Edit", then enter the detail form of the QoS rule. Click "**Apply**" after editing the form and the rule will be saved.

Adjust QoS rule priority You can select the rule and click "Move Up" to make its priority higher. You also can select the rule and click "Move Down" to make its priority lower.

15 TOOLBOX Settings

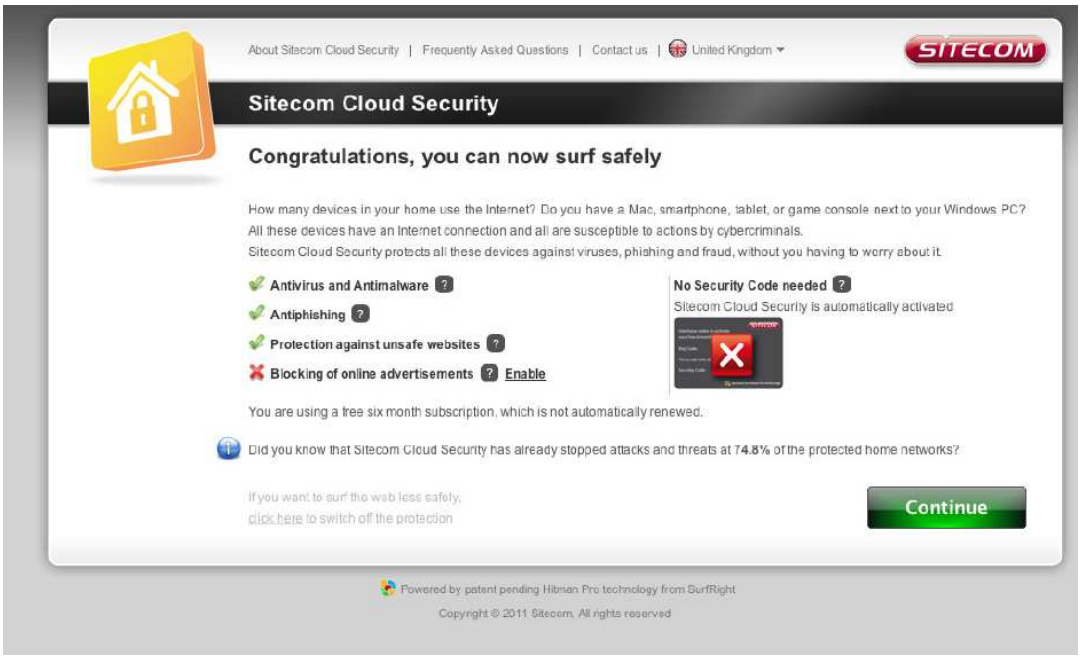
Sitecom Cloud Security

Antivirus software alone is not safe enough. You can now benefit from additional built-in security in your modem or router. Protect all devices in your home network against cybercrime while browsing. Activated automatically, your network and devices are better secured than ever before.

Your Sitecom device comes with a 6 month free *Sitecom cloud security* subscription.

After you have set up your Sitecom device for internet access, open the webbrowser and enter http://www.sitecomcloudsecurity.com in the address bar.

If the device has been properly configured the following web page should be shown.

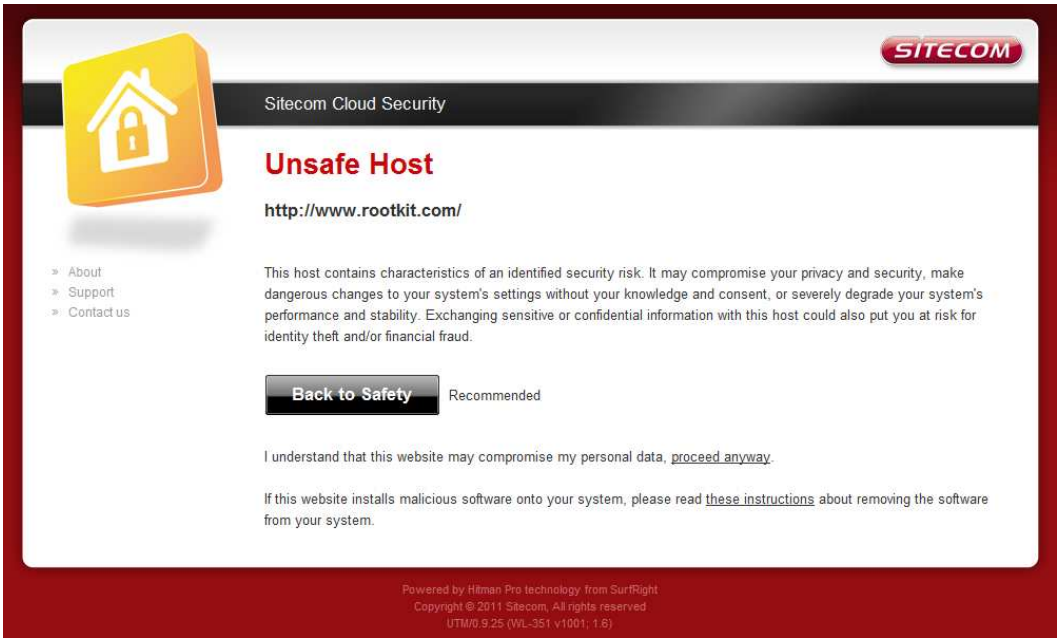

About Sitecom Cloud Security | Frequently Asked Questions | Contact us | United Kingdom
SITECOM
Sitecom Cloud Security
Congratulations, you can now surf safely
How many devices in your home use the Internet? Do you have a Mac, smartphone, tablet, or game console next to your Windows PC?
All these devices have an Internet connection and all are susceptible to actions by cybercriminals.
Sitecom Cloud Security protects all these devices against viruses, phishing and fraud, without you having to worry about it.
Antivirus and Antimalware
Antiphishing
Protection against unsafe websites
Blocking of online advertisements
Enable
No Security Code needed
Sitecom Cloud Security is automatically activated
You are using a free six month subscription, which is not automatically renewed.
Did you know that Sitecom Cloud Security has already stopped attacks and threats at 74.8% of the protected home networks?
If you want to surf the web less safely,
click here to switch off the protection
Continue
Powered by patent pending Hitman Pro technology from SurfRight
Copyright © 2011 Sitecom. All rights reserved

Here you can see which security features are activated.

The *Sitecom Cloud Security* service offers the following protection options:

- Anti-Malware
- Anti-Phishing
- Protection against unsafe websites
- Advertisement blocking

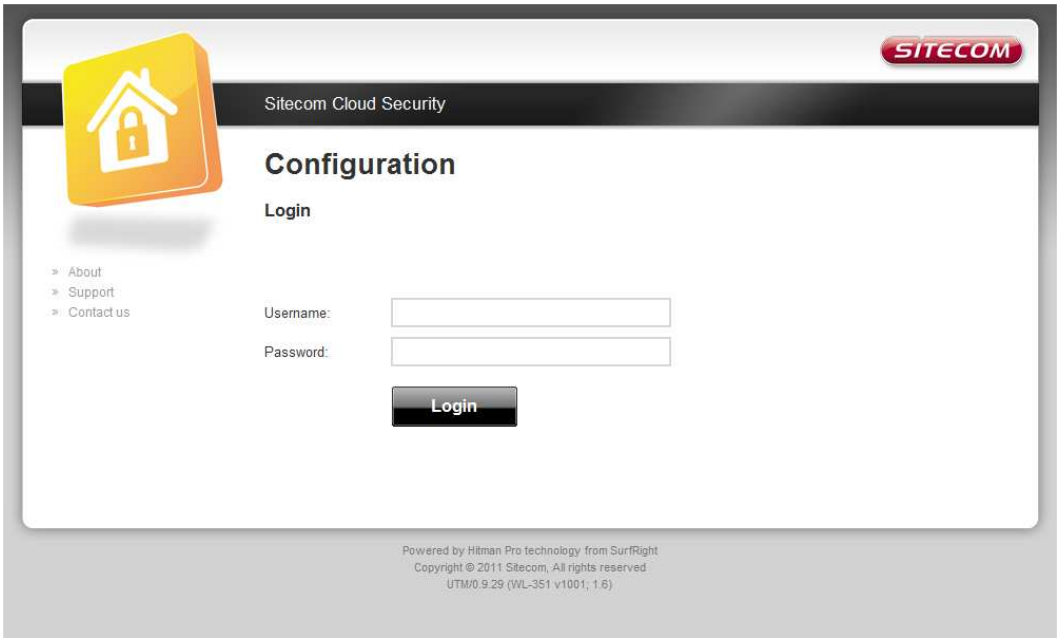
With the protection of *unsafe websites* activated the S*itecom Cloud Security* will always check if a website is safe. If it is not safe it will inform you that is not safe to enter.


SITECOM
Sitecom Cloud Security
Unsafe Host
http://www.rootkit.com/
» About
» Support
» Contact us
This host contains characteristics of an identified security risk. It may compromise your privacy and security, make dangerous changes to your system's settings without your knowledge and consent, or severely degrade your system's performance and stability. Exchanging sensitive or confidential information with this host could also put you at risk for identity theft and/or financial fraud.
Back to Safety
Recommended
I understand that this website may compromise my personal data, proceed anyway.
If this website installs malicious software onto your system, please read these instructions about removing the software from your system.
Powered by Hitman Pro technology from SurfRight
Copyright © 2011 Sitecom, All rights reserved
UTM/0.9.25 (WL-351 v1001; 1.6)

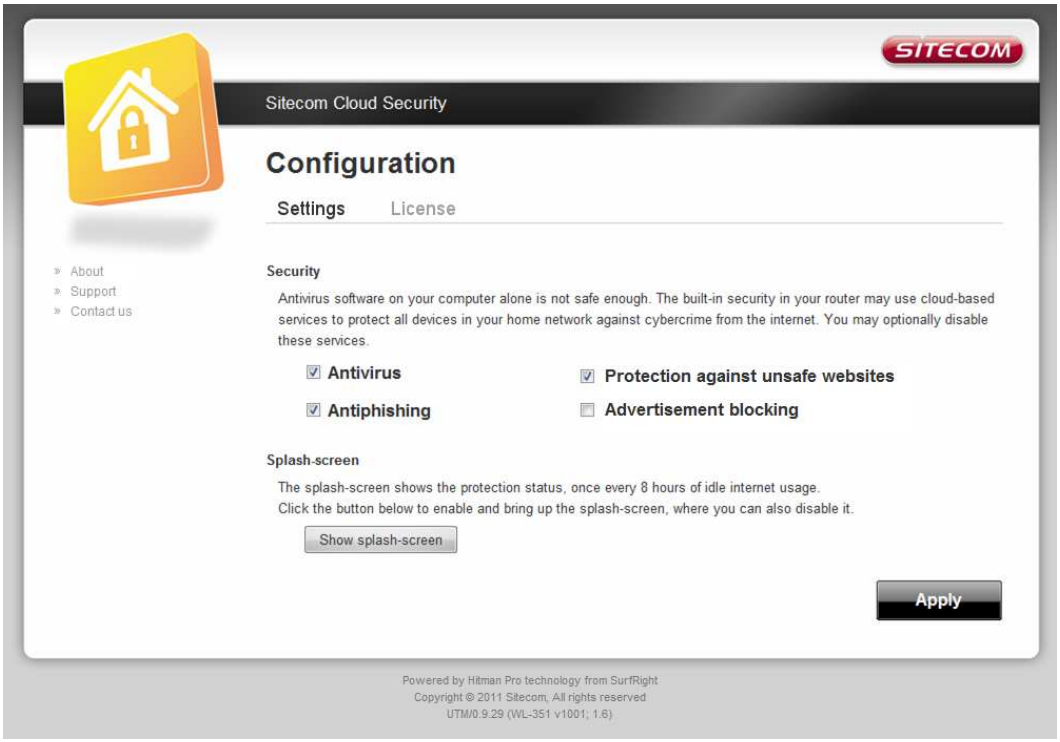
If you still wish to visit this webpage click on 'proceed anyway'. Alternatively click 'Back to Safety' so that your security will not be breached.

If you wish to change your security options or to extend your subscription at any time, open http://www.sitecomcloudsecurity.com from your web browser.

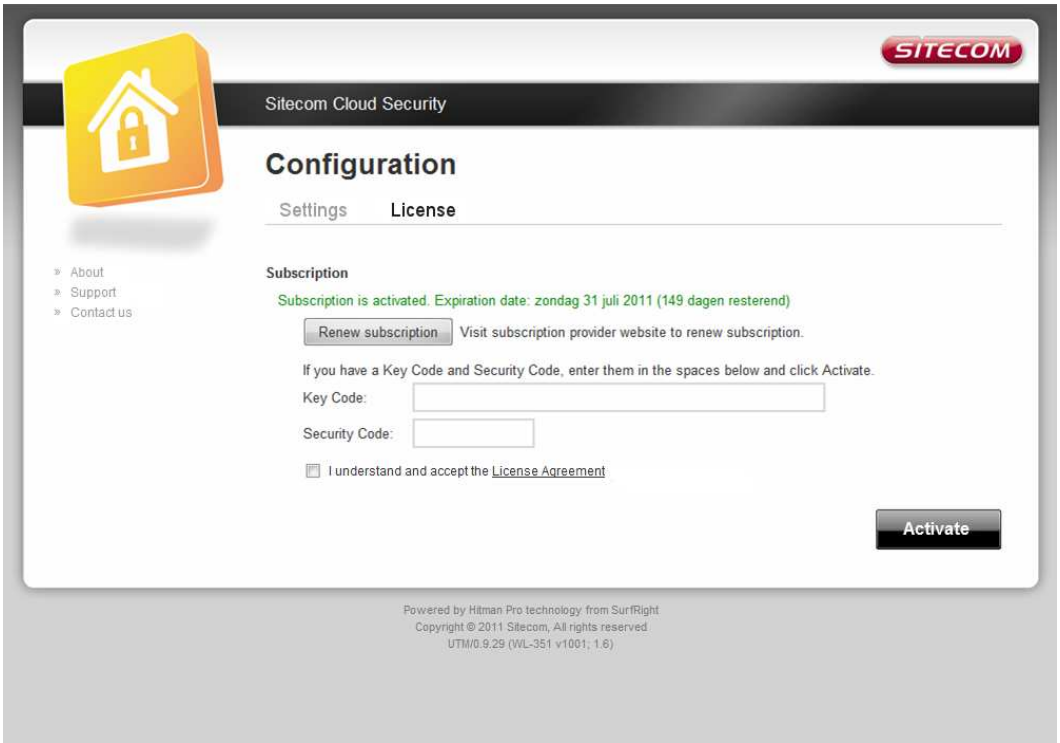
You will be asked for a username and password. These can be found on the backlabel on the bottom of your Sitecom router or modem.



If the login succeeded you can click on 'Settings' to change your security options.


SITECOM
Sitecom Cloud Security
Configuration
Settings
License
About
Support
Contact us
Security
Antivirus software on your computer alone is not safe enough. The built-in security in your router may use cloud-based services to protect all devices in your home network against cybercrime from the internet. You may optionally disable these services.
Antivirus
Protection against unsafe websites
Antiphishing
Advertisement blocking
Splash-screen
The splash-screen shows the protection status, once every 8 hours of idle internet usage.
Click the button below to enable and bring up the splash-screen, where you can also disable it.
Show splash-screen
Apply
Powered by Hitman Pro technology from SurfRight
Copyright © 2011 Sitecom, All rights reserved
UTM/0.9.29 (WL-351 v1001; 1.6)

Or click 'License' to renew your subscription.


SITECOM
Sitecom Cloud Security
Configuration
Settings
License
About
Support
Contact us
Subscription
Subscription is activated. Expiration date: zondag 31 juli 2011 (149 dagen resterend)
Renew subscription
Visit subscription provider website to renew subscription.
If you have a Key Code and Security Code, enter them in the spaces below and click Activate.
Key Code:
Security Code:
I understand and accept the License Agreement
Activate
Powered by Hitman Pro technology from SurfRight
Copyright © 2011 Sitecom, All rights reserved
UTM/0.9.29 (WL-351 v1001; 1.6)

If you wish to disable to Sitecom cloud security at any time, open the webpage of your Sitecom product and log in with the supplied credentials (these can be

found on the back label on the bottom of your Sitecom device).

Go to Toolbox and select “Sitecom Cloud Security”.

Click the “Disable” radio button and click ‘Apply’ for the settings to take effect.

Password change options

You can change the password required to log into the broadband router's system web-based management. Passwords can contain 0 to 12 alphanumeric characters, and are case sensitive.

Current Password Fill in the current password to allow changing to a new password.

New Password Enter your new password.

Confirm Password Enter your new password again for verification purposes.

Click <**Apply**> at the bottom of the screen to save the above configurations

Time Zone

The Time Zone allows your router to base its time on the settings configured here, which will affect functions such as Log entries and Firewall settings.

Set Time Zone Select the time zone of the country you are currently in. The router will set its time based on your selection.

Time Server Address You can set an NTP server address.

Enable Daylight Savings The router can also take Daylight savings into account. If you wish to use this function, you must check/tick the enable box to enable your daylight saving configuration (below).

Start Daylight Savings Time Select the period in which you wish to start daylight Savings Time

End Daylight Savings Time Select the period in which you wish to end daylight Savings Time

Click <**Apply**> at the bottom of the screen to save the above configurations

Remote Management

The remote management function allows you to designate a host in the Internet the ability to configure the Broadband router from a remote site. Enter the designated host IP Address in the Host IP Address field.

Host Address This is the IP address of the host in the Internet that will have management/configuration access to the Broadband router from a remote site. If the Host Address is left 0.0.0.0 this means anyone can access the router's web-based configuration from a remote location, providing they know the password.

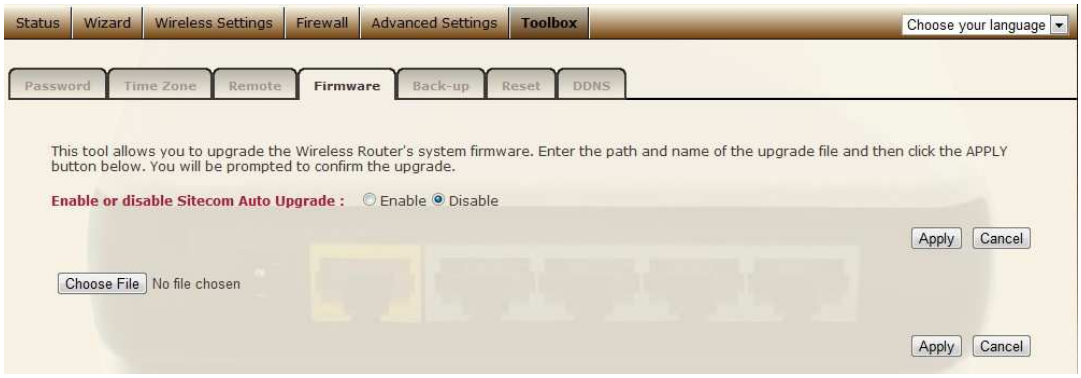
Port The port number of the remote management web interface.

Check "**Enabled**" to enable the remote management function.

Click <**Apply**> at the bottom of the screen to save the above configurations.

Firmware Upgrade

This page allows you to upgrade the router's firmware.



Enable or disable Sitecom Auto Upgrade if Enabled the router will automatically check for firmware updates. If a new firmware has been detected a pop/up will appear in the webbrowser and inform the user about the new firmware and the changes and allows to Install the update.
Select **Enable** or **Disable** and click apply for the settings to take effect.

Firmware Upgrade This tool allows you to upgrade the Broadband router's system firmware. To upgrade the firmware of your Broadband router, you need to download the firmware file to your local hard disk, and enter that file name and path in the appropriate field on this page. You can also use the Browse button to find the firmware file on your PC.

Once you've selected the new firmware file, click <**Apply**> at the bottom of the screen to start the upgrade process.

Backup Settings

The Backup screen allows you to save (Backup) the router's current configuration settings. When you save the configuration setting (Backup) you can re-load the saved configuration into the router through the Restore selection. If extreme problems occur you can use the Restore to Factory Defaults selection, this will set all configurations to its original default settings (e.g. when you first purchased the router).

Status
Wizard
Wireless Settings
Firewall
Advanced Settings
Toolbox
Choose your language
Password
Time Zone
Remote
Firmware
Back-up
Reset
DDNS
Use the "Backup" tool to save the Wireless Router's current configuration to a file named "config.bin". You can then use the "Restore" tool to restore the saved configuration to the Wireless Router. Alternatively, you can use the "Restore to Factory Default" tool to force the Wireless Router to perform a system reset and restore the original factory settings.
Restore to Factory Default :
Reset
Backup Settings :
Save
Restore Settings :
Choose File
No file chosen
Upload

Use the "Backup" tool to save the Broadband router current configuration to a file named "**config.bin**" on your PC. You can then use the "Restore" tool to restore the saved configuration to the Broadband router. Alternatively, you can use the "Restore to Factory Defaults" tool to force the Broadband router to perform a power reset and restore the original factory settings.

Reset

You can reset the router's system should any problem exist. The reset function essentially re-boots your router's system.

Status
Wizard
Wireless Settings
Firewall
Advanced Settings
Toolbox
Choose your language
Password
Time Zone
Remote
Firmware
Back-up
Reset
DDNS
In the event the system stops responding correctly or stops functioning, you can perform a reset. Your settings will not be changed. To perform the reset, click on the APPLY button. You will be asked to confirm your decision. The reset will be completed when the LED Power light stops blinking.
Apply

DDNS

DDNS allows you to map the static domain name to a dynamic IP address. You must get an account, password and your static domain name from the DDNS service providers. This router supports DynDNS, TZO and other common DDNS service providers.

Enable/Disable Enable or disable the DDNS function of this router

Provider Select a DDNS service provider

Domain name Fill in your static domain name that uses DDNS

Account/E-mail The account that your DDNS service provider assigned to you

Password/**Key** The password you set for the DDNS service account above

Click <**Apply**> at the bottom of the screen to save the above configurations.

Parts of the firmware of the WLR-2100/3100 Wireless Broadband Router are subject to the GNU general public license.

Appendix A: Licensing Information

This product includes third-party software licensed under the terms of the GNU General Public License. You can modify or redistribute this free software under the terms of the GNU General Public License. Please see Appendix B for the exact terms and conditions of this license.

Specifically, the following part of this product is subject to the GNU GPL:

#	Package name	Source
1	Linux v2.6.34.5	www.kernel.org
2	busybox v1.7.5	http://www.busybox.net/
3	termcap v1.3.1	ftp://ftp.gnu.org/gnu/termcap
4	libupnp v1.6.0	http://pupnp.sourceforge.net/
5	pcre v6.x	http://www.pcre.org/
6	popt v1.7	http://freecode.com/projects/popt
7	dnsmasq v2.39	http://thekelleys.org.uk/dnsmasq/doc.html
8	iproute2 v2.6.16	http://www.linuxfoundation.org/en/Net:Iproute2
9	rp-pppoe v3.8	http://www.roaringpenguin.com/products/pppoe
10	iptables v1.4.4	http://www.netfilter.org/projects/iptables/index.html
11	flex v2.5.35	http://flex.sourceforge.net
12	linuxigd v1.0	http://linux-igd.sourceforge.net/index.php
13	wireless_tools v28	http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html
14	hostapd v0.7.3	http://hostap.epitest.fi/
15	igmpproxy v0.1-beta2	http://sourceforge.net/projects/igmpproxy
16	pptp-client v1.7.1	http://pptpclient.sourceforge.net/
17	accel-pptp/pppd-plugin v0.8.3-rc5	http://accel-pptp.sourceforge.net/
18	ppp v2.4.3	http://ppp.samba.org/
19	udhcp v0.9.9-pre	http://sources.busybox.net/index.py/trunk/udhcp-web/index.html?revision=9967
20	ez-ipupdate v3.0.11b8	http://ez-ipupdate.com
21	uboot v1.1.4	http://www.denx.de/wiki/U-Boot
22	gcc v4.3.4	http://gcc.gnu.org/
23	uclibc v0.9.29	http://www.uclibc.org
24	zlib v1.2.3	http://www.zlib.net/
25	mtd-utils v1.2	http://git.infradead.org
26	radvd v1.6	http://www.litech.org/radvd/

Availability of source code

Sitecom Europe BV has made available the full source code of the GPL licensed software, including any scripts to control the compilation and installation of the object code in the driver section of this product on the Sitecom website.

No Warranty

The free software included in this product is distributed in the hope that it will be useful, but WITHOUT ANY LIABILITY OF OR ANY WARRANTY FROM THE LICENSOR.

Appendix B: GNU GENERAL PUBLIC LICENSE

Version 2, June 1991 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too. When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things. To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights. We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations. Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all. The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1.

You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2.

You may modify your copy or copies of the Program or any portion of it, thus forming a work

based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions: a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change. b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License. c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.
3.
You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following: a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.
4.
You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
5.
You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.
6.
Each time you redistribute the Program (or any work based on the Program), the recipient

automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
7.
If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.
8.
If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
9.
The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.
10.
If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11.
BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
12.
IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE

PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Certifications

CE/LVD

· EN 60950-1: 2006+A11 (2009)

CE/EMC

· EN 301 489-1 V1.8.1

· EN 301 489-17 V2.1.1

RADIO SPECTRUM

· EN 300 328 V1.7.1 2006-10

· EN 50385 2002

www.sitecom.com